C2M2 | Cybersecurity Capability Maturity Model

PDF-Based Tool User Guide

User Guide for the PDF-Based Self-Evaluation Tool C2M2 Version 2.1

June 2022

U.S. DEPARTMENT OF ENERGY | Office of Cybersecurity, Energy Security, and Emergency Response

TABLE OF CONTENTS

LIST OF FIGURES

TABLE OF CONTENTS

This material is based upon work funded and supported by the Department of Energy under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

DM22-0585

1. INTRODUCTION

The Cybersecurity Capability Maturity Model (C2M2) focuses on the implementation and management of cybersecurity practices associated with information technology (IT), operations technology (OT), and information assets and the environments in which they operate. The model can be used to:

- strengthen the cybersecurity capabilities of organizations
- enable organizations to effectively and consistently evaluate and benchmark cybersecurity capabilities
- share knowledge, best practices, and relevant references across organizations to improve cybersecurity capabilities
- enable organizations to prioritize actions and investments to improve cybersecurity capabilities

The C2M2 model document describes a self-evaluation methodology that an organization can use to evaluate its cybersecurity capabilities consistently, to communicate its capability levels in meaningful terms, and to inform the prioritization of its cybersecurity investments. The C2M2 V2.1 PDF-Based Self-Evaluation Tool ("the Tool") supports this methodology by providing a mechanism to capture and report upon the implementation levels of an organization's cybersecurity capabilities. For more detailed information, refer to Section 5, "Using the Model," in *Cybersecurity Capability Maturity Model (C2M2) V2.1*.

In addition to the C2M2 V2.1 PDF-Based Self-Evaluation Tool, the Department of Energy (DOE) has also made a C2M2 V2.1 HTML-based Self-Evaluation tool available to perform self-evaluations. These tools were designed to be interoperable and exported results of a self-evaluation can be imported into either tool.

1.1 Purpose

This guide is intended to help users of the Tool complete a self-evaluation, in conjunction with guidance from *Cybersecurity Capability Maturity Model V2.1* and *C2M2 V2.1 Self-Evaluation Guide*. This document describes:

- requirements for using the Tool
- Tool navigation and access features
- report generation and interpretation
- comparison of self-evaluations

1.2 Data Privacy

All data entered in the Tool are retained locally on the user machine. No data are sent to external parties (e.g., DOE, regulatory bodies). Users have full control over the information and can export it. Organizations should consider safeguards for the data input into the Tool and follow organizational and critical infrastructure protection requirements.

1.3 System Requirements

The Tool is a PDF document and requires either Adobe Acrobat or Adobe Reader, Version 8 or higher.

2. TOOL USAGE PROCESS

This section describes:

- setup to be completed prior to using the Tool during a self-evaluation,
- how to use the Tool during a self-evaluation,
- how to generate a report, and
- how to use the data import and export functions.

2.1 Initial Setup

Before using the Tool to complete a self-evaluation or to hold a self-evaluation workshop, complete the following setup steps.

1. Send an email to C2M2@hq.doe.gov to request the C2M2 V2.1 PDF-Based Self-Evaluation Tool.
2. Save the PDF document attached to the email response you receive to a local storage device before opening it. Opening the file directly from the email can cause limited functionality.
3. Open the PDF document in Adobe Acrobat or Adobe Reader, Version 8 or higher.
4. Click **Enable All Features** in the top-left of the window. The report will not function if all features are not enabled.

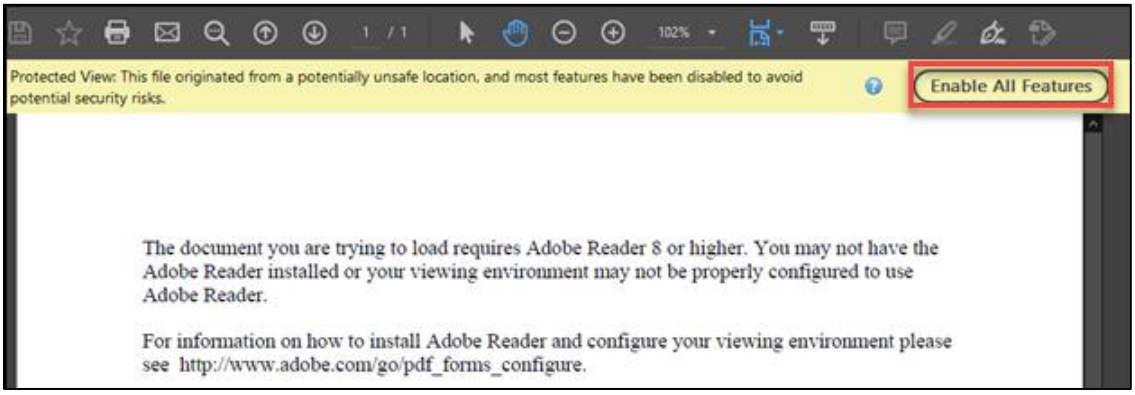


Figure 1 - Enable All Features Button

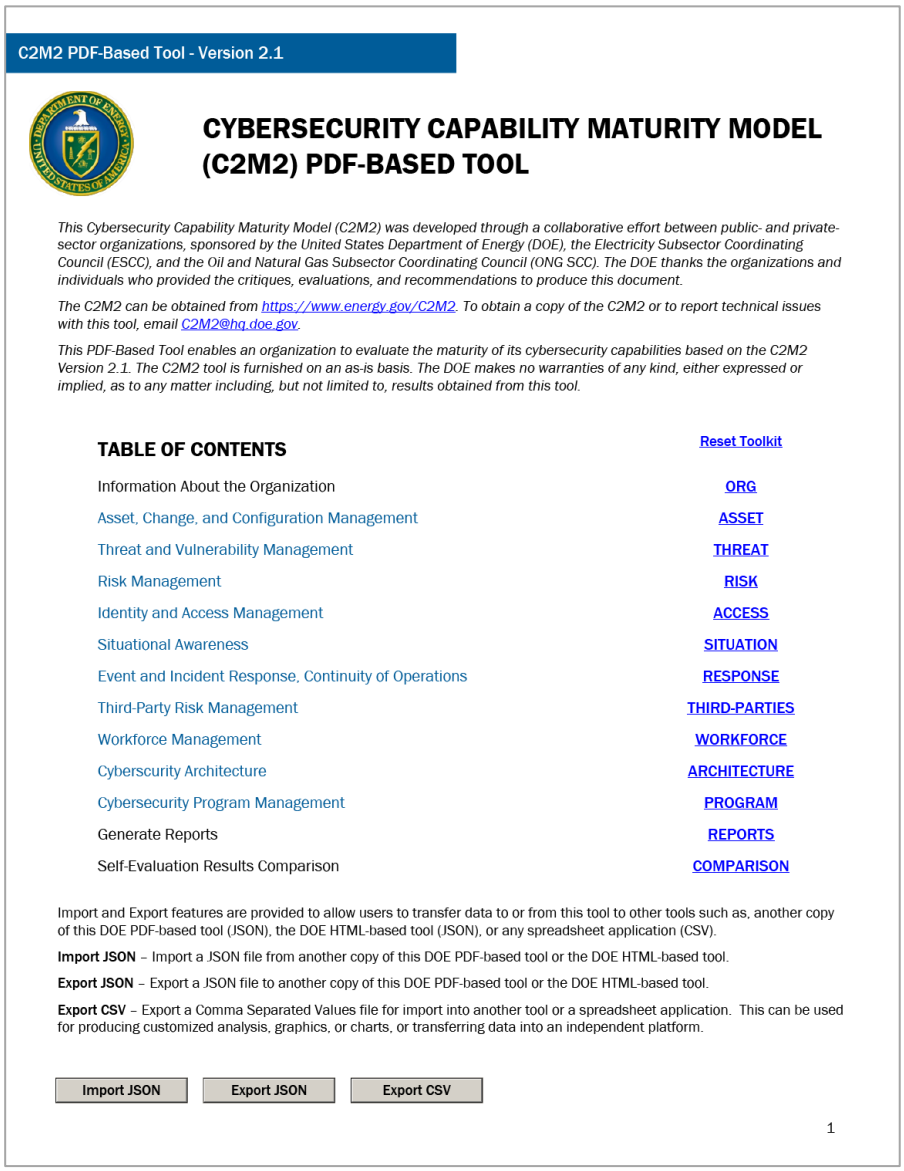
5. When the cover of *Self-Evaluation Tool, Version 2.1* appears, the file is enabled and ready for use.

Figure 2 - Cover of the C2M2 Self-Evaluation Tool

2.2 Table of Contents and Information About the Organization

The **Table of Contents (TOC) Page** lists helpful links, as well as access to more advanced features available in the Tool.

- Page 1 shows the **Table of Contents Page** with a link to the right of each domain name.



C2M2 PDF-Based Tool - Version 2.1

CYBERSECURITY CAPABILITY MATURITY MODEL (C2M2) PDF-BASED TOOL

This Cybersecurity Capability Maturity Model (C2M2) was developed through a collaborative effort between public- and private-sector organizations, sponsored by the United States Department of Energy (DOE), the Electricity Subsector Coordinating Council (ESCC), and the Oil and Natural Gas Subsector Coordinating Council (ONG SCC). The DOE thanks the organizations and individuals who provided the critiques, evaluations, and recommendations to produce this document.

The C2M2 can be obtained from https://www.energy.gov/C2M2. To obtain a copy of the C2M2 or to report technical issues with this tool, email C2M2@hq.doe.gov.

This PDF-Based Tool enables an organization to evaluate the maturity of its cybersecurity capabilities based on the C2M2 Version 2.1. The C2M2 tool is furnished on an as-is basis. The DOE makes no warranties of any kind, either expressed or implied, as to any matter including, but not limited to, results obtained from this tool.

TABLE OF CONTENTS Reset Toolkit

Information About the Organization	ORG
Asset, Change, and Configuration Management	ASSET
Threat and Vulnerability Management	THREAT
Risk Management	RISK
Identity and Access Management	ACCESS
Situational Awareness	SITUATION
Event and Incident Response, Continuity of Operations	RESPONSE
Third-Party Risk Management	THIRD-PARTIES
Workforce Management	WORKFORCE
Cyberscurity Architecture	ARCHITECTURE
Cybersecurity Program Management	PROGRAM
Generate Reports	REPORTS
Self-Evaluation Results Comparison	COMPARISON

Import and Export features are provided to allow users to transfer data to or from this tool to other tools such as, another copy of this DOE PDF-based tool (JSON), the DOE HTML-based tool (JSON), or any spreadsheet application (CSV).

Import JSON – Import a JSON file from another copy of this DOE PDF-based tool or the DOE HTML-based tool.

Export JSON – Export a JSON file to another copy of this DOE PDF-based tool or the DOE HTML-based tool.

Export CSV – Export a Comma Separated Values file for import into another tool or a spreadsheet application. This can be used for producing customized analysis, graphics, or charts, or transferring data into an independent platform.

Import JSON | Export JSON | Export CSV

1

Figure 3 - Tool Table of Contents

- Click the **Reset Toolkit** link to remove **all** responses that have been entered. This feature is useful to start a new evaluation.
- Data import and export functions are on the bottom-left of the page. See Section 2.7 "Data Import and Export" for more information.

2.3 Information About the Organization

The Tool provides the user with three fields to enter general information that is helpful for individuals who were not present at a self-evaluation workshop or for later report review.

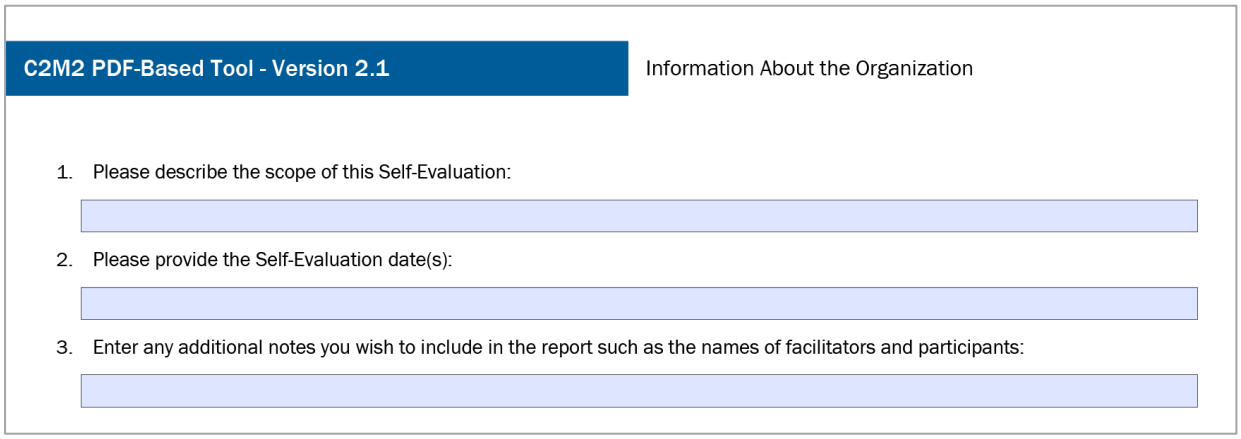


Figure 4 - Information About the Organization

Each field shown in Figure 4 must be completed to generate a report after completion of the self-evaluation.

- Field 1 **Description**: Documents the scope or function of the self-evaluation. Identification of the function is an essential step in the self-evaluation process. The description of the scope of the self-evaluation helps readers of the report interpret responses accurately and helps in planning follow-on activities.
- Field 2 **Self-Evaluation Date**: Lists the dates of the self-evaluation. Understanding the date of the self-evaluation helps readers interpret the results and can be useful when comparing the results to a future self-evaluation.
- Field 3 **Additional Notes**: Provides information that the workshop facilitators and participants consider to be useful. Because the self-evaluation is a point-in-time view of the function, use this field to document facilitators, participants, high-level considerations, notes, and constraints. This information helps with follow-on activities and provides additional context of the SME responses.

2.4 Performing the Self-Evaluation

The **Domain Introduction Section** details the domain purpose statement, the domain objectives, and the domain description. This information helps self-evaluation workshop participants understand the focus of the domain.

The **Objectives and Practices Section** is used to input the implementation level of each practice and associated notes for each domain objective, as well as practice-level guidance and key terms.

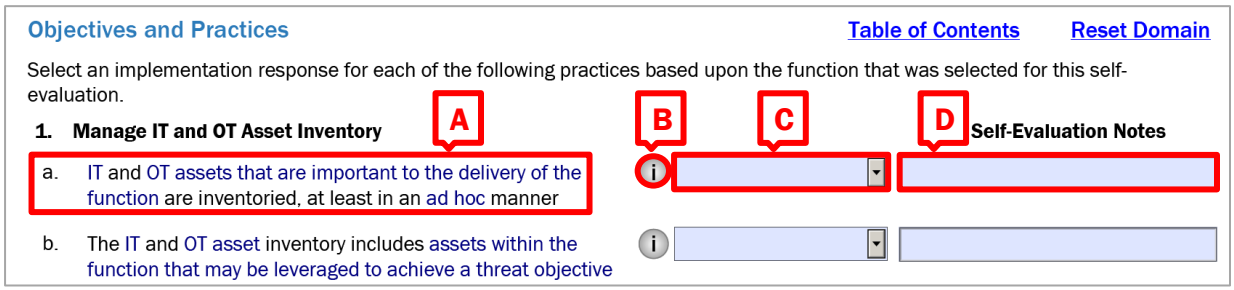


Figure 5 – Objectives and Practices Section

The **Objectives and Practices Section** contains the following items:

- **Table of Contents** button navigates to the first page of the Tool and can be used to navigate quickly between model domains.
- **Reset Domain** button is used to remove all responses that have been entered for the current domain.
- **Practices by Objective** provides the C2M2 practices grouped by objective. As shown in Figure 5, each practice contains the following:
  - **A: Practice Text** defines an activity that supports a domain objective.
  - **B: Help Text** displays or hides help text specific to the practice.
  - **C: Practice Implementation** provides implementation responses from a drop-down menu. Users select the response that best represents the current state of implementation. A response must be selected for every practice to generate a report after completion of the self-evaluation.
  - **D: Self-Evaluation Notes** provides a space to capture details that influence and support the selection of an answer, considerations for future remediation, or other pertinent information. This field is particularly useful when the report is reviewed at a later date, because details can be entered that provide justification for the selection of an implementation level. This field supports alphanumerical and special characters. This is not a required field, but highly recommended.
- **Glossary Terms** provides descriptions of key terms in each practice. Terms with definitions are shown in "blue" text. Hover over a term to display the definition in a pop-up, as shown in Figure 6. Click a term to display the definition in a window below the practice, as shown in Figure 7. Click the term a second time or click the "x" in the top right to close the definition window.

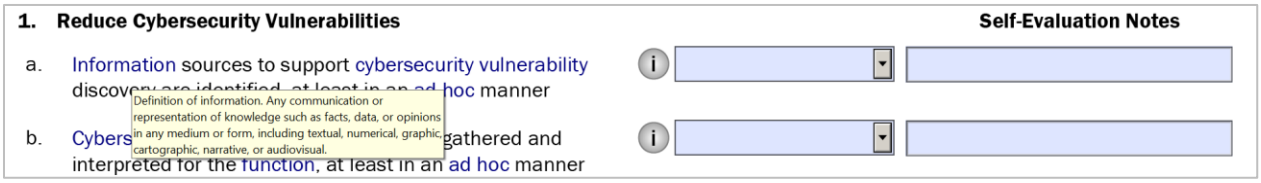


Figure 6 - Practice Glossary Definition Pop-Up

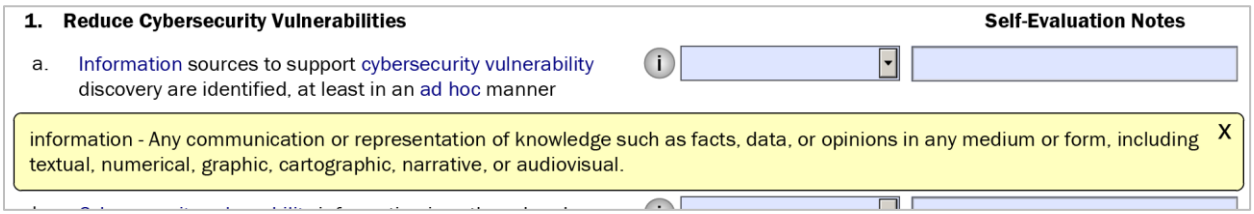


Figure 7 - Practice Glossary Definition Window

2.5 Report Generation

After completing a self-evaluation, a report can be generated with information that helps identify gaps in cybersecurity capabilities. Prioritized plans can then be developed to close the gaps. The report includes visualizations and details from the responses input during the self-evaluation.

IMPORTANT: Before a report can be generated, the three organization information fields, shown in Figure 4 must be completed, and responses must be selected for the implementation level for all practices, shown in Figure 5, Item C.

To generate a report, click **Generate Report** on the final page of the self-evaluation, as shown in Figure 9, Item A. The generation process may take up to five minutes; a pop-up dialog box indicates the progress of the report.

IMPORTANT: Do not close the application while the report is being generated.

2.6 Revising Self-Evaluation Responses

Self-evaluation responses can be revised after report generation. As shown in Figure 8, from the Table of Contents, click **Edit Self-Evaluation** in the top-right, then revise the responses.

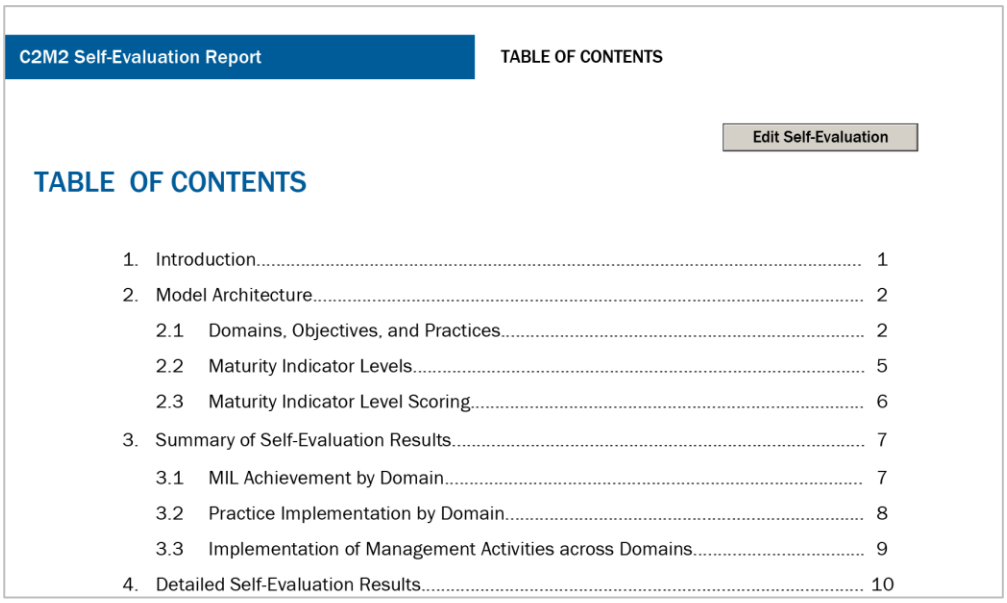


Figure 8 - Report Table of Contents (TOC)

2.7 Data Import and Export

The C2M2 Tool allows the import and export data. These features enable information sharing and interoperability with other tools and applications. In addition to the Generate Report button, the final page of the self-evaluation includes the following functions for data import and export, as shown in Figure 9.

- **B: Import JSON File** imports an existing JSON file into the Tool. This feature supports JSON files exported by both the PDF-Based Self-Evaluation Tool and the HTML-Based Self-Evaluation Tool.
- **C: Export JSON File** creates a structured file that contains all responses input into the Tool. This feature generates JSON files that can be imported by both the PDF-Based Self-Evaluation Tool and the HTML-Based Self-Evaluation Tool.
- **D: Export CSV File** generates a comma-separated-values (CSV) file that can be used with other tools or in a spreadsheet application. Typically, such an application enables you to perform analysis and develop graphics or charts.

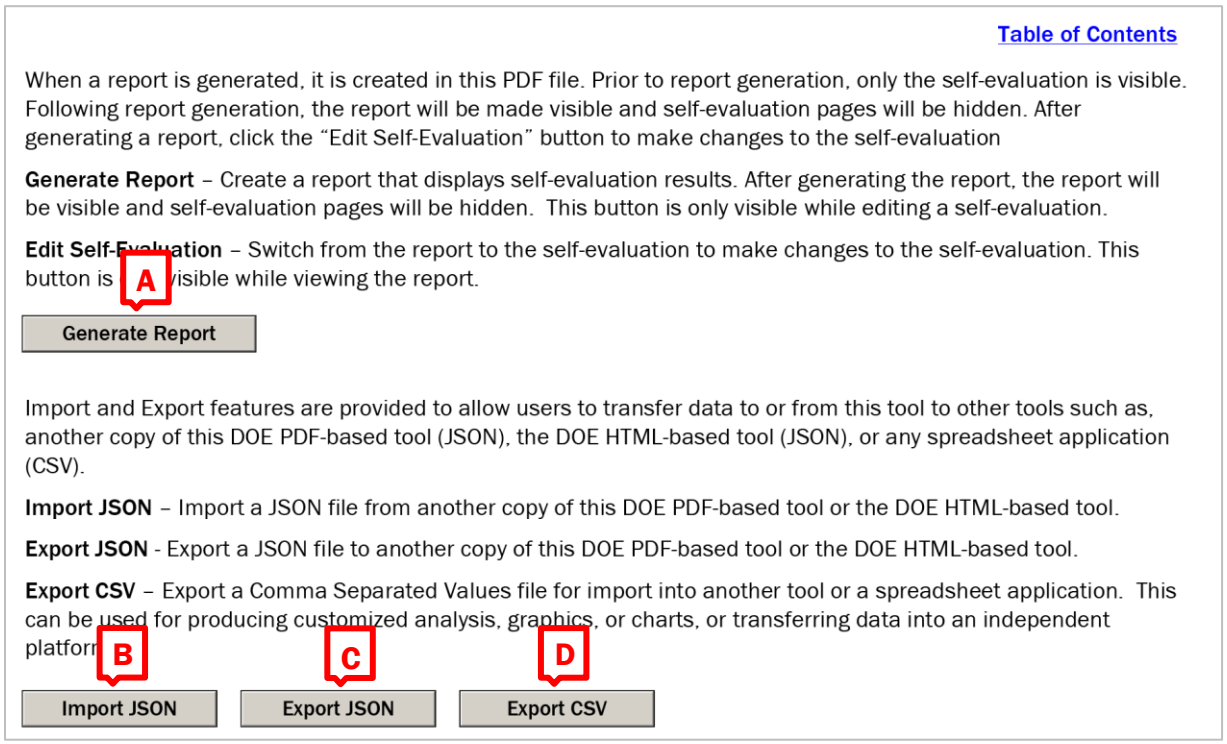


Figure 9 - Report Generation, Data Import and Export

2.8 Self-Evaluation Results Comparison

The Self-Evaluation Results Comparison feature allows the comparison of up to five self-evaluations, including the current self-evaluation. Users may choose to compare C2M2 V2.0 or C2M2 V2.1 self-evaluations, but all data sets must be from the same version. JSON files from either the C2M2 V2.1 PDF-Based Self-Evaluation Tool or the C2M2 V2.1 HTML-Based Self-Evaluation Tool can be loaded for comparison.

As shown in Figure 10, the **Self-Evaluation Results Comparison** section contains the following items:

- **Table of Contents** button navigates to the first page of the Tool and can be used to navigate quickly between model domains.
- **Load Data Sets** section contains the following items:
  - **A: Data Set Description** defines the description for each imported data set. For example, the function that was evaluated when comparing different functions or the date of the self-evaluation for comparing the same function over a series of time.
  - **B: Import JSON buttons** are used to import each individual JSON file that will be compared. For each self-evaluation, click **Import JSON** and select the JSON file.

- **C: Select Model Version** is used to select the C2M2 version of the imported data sets.
- **D: Use Current Data Set** can be checked if to use the self-evaluation responses currently in the tool as one of the data sets.
- **E: Generate Comparison** generates the comparison report.

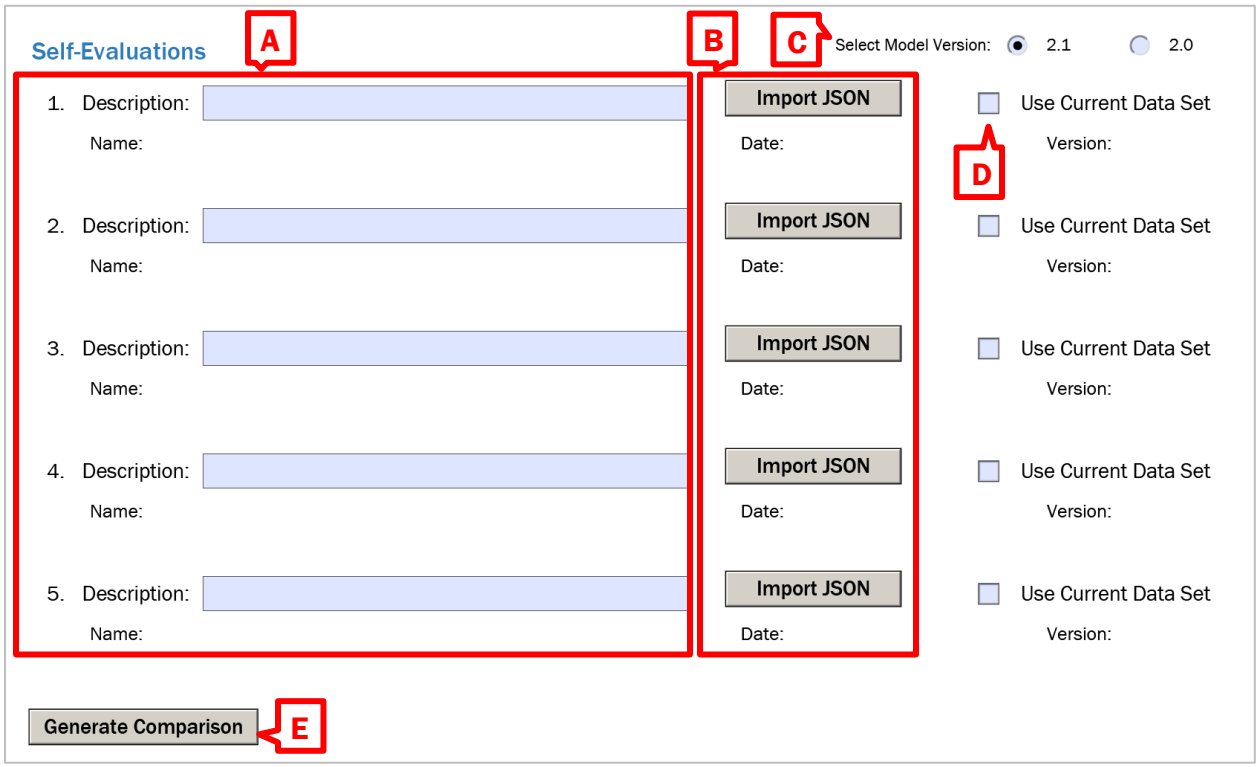


Figure 10 - Self-Evaluation Comparison Data Set Import

After a JSON file is imported, the Tool will populate the "Name" and "Date" fields with organization information that was entered into the Tool when the self-evaluation was completed (see the Information About the Organization section for more information) and the Tool will display "Import Successful," as shown in Figure 11. The "Name" field corresponds with **Description** and "Date" field corresponds with the **Self-Evaluation Date** from the JSON file. The "Version" field corresponds with the C2M2 version of the Tool.

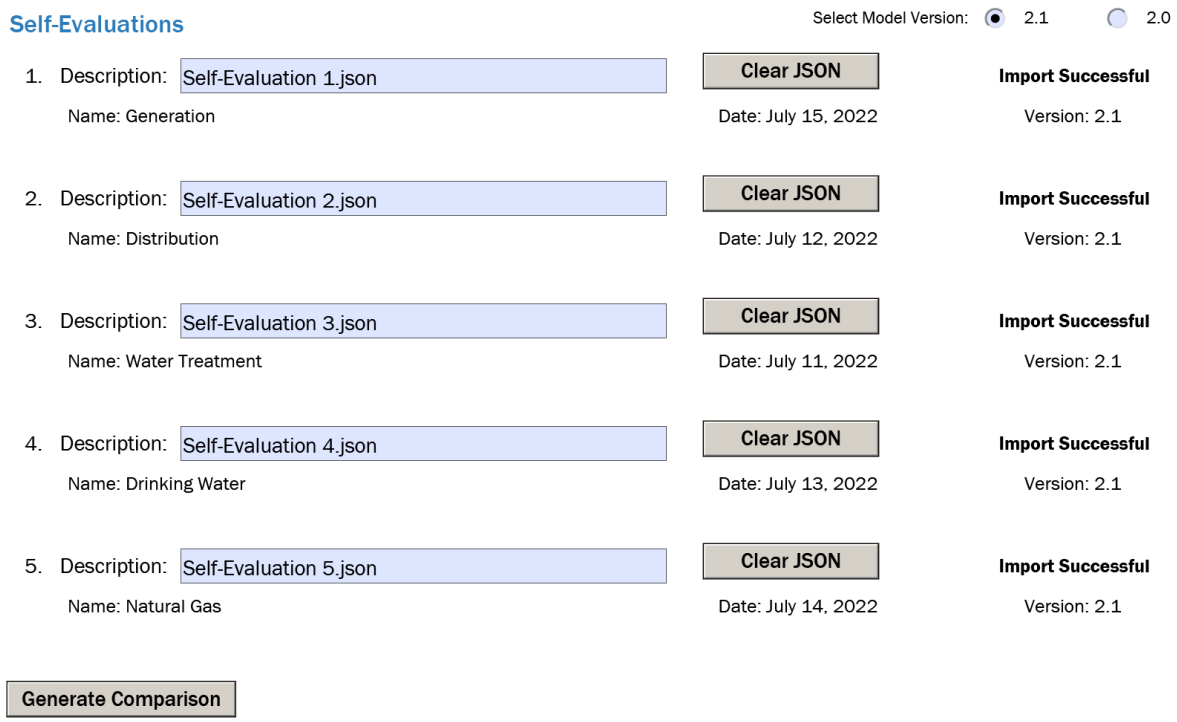


Figure 11 - Successful Import of Five Data Sets

To load a different JSON file, click the **Clear JSON** button and repeat the previously described process to import a JSON file. To generate a report, click **Generate Comparison** at the bottom of the **Self-Evaluation Results Comparison** section, as shown in Figure 11. The generation process may take up to five minutes; a pop-up dialog box indicates the progress of the report.

3. INTERPRETING THE SELF-EVALUATION REPORT

Self-evaluation tool reports provide useful information for stakeholders at different levels of the organization. Detailed information is intended for practitioners, and summary reporting is available for communicating with organizational leadership. This section provides a high-level overview of the sections of the report. Refer to the introductory information in each report section for a more detailed explanation and for potential uses of the information.

3.1 Section 1 – Introduction

Section 1 includes the organizational information entered during the self-evaluation:

- scope (function) of the self-evaluation
- date(s) of the self-evaluation
- additional notes

3.2 Section 2 – Model Architecture

Facilitators and Subject Matter Experts (SMEs) gain a general understanding of the C2M2 model after completing a self-evaluation. However, Section 2 documents information on the model architecture, which gives all readers a baseline knowledge useful in the interpretation of the reports in the subsequent sections. Section 2 provides:

- information on the structure of the model (domains, objectives, and practices),
- descriptions of the domains,
- an explanation of the MIL scale, and
- a description of the process used to determine the implementation level during the self-evaluation.

3.3 Section 3 – Summary of Self-Evaluation Results

Section 3 contains high-level graphical depictions of the self-evaluation results. The graphics are a summary view of overall implementation level, and a focused view of the management practices.

- The “MIL Achievement by Domain” graphic provides a high-level overview of the MIL achieved for each domain based on the implementation responses recorded during the self-evaluation.

- The "Practice Implementation by Domain" graphic may be a useful starting point to determine cybersecurity capability implementation gaps by reviewing performance by domain or MIL.
- The "Implementation of Management Activities Across Domains" graphic aids in understanding the management activities across the domains; gaps in implementation may indicate areas where improvement would increase institutionalization of cybersecurity capabilities.

3.4 Section 4 – Detailed Self-Evaluation Results

Section 4 contains results for each domain at three levels: objective, MIL, and practice. This information provides a detailed understanding of the implementation level of each practice within a domain and helps identify gaps in implementation at the objective level.

After analyzing the data in Section 3, this section can be used to gain insight into gaps identified at the MIL or domain level. For example, if the performance of a domain appears out of alignment with the organization's cybersecurity objectives, a review of this section can help determine actions to be taken to improve the implementation level of domain activities.

3.5 Section 5 – Using the Self-Evaluation Results

Section 5 introduces a potential approach for using the model and the Tool, as illustrated in Figure 12.

- **Step 1: Perform a Self-Evaluation** – This step is accomplished by using the Tool to complete a self-evaluation.
- **Step 2: Analyze Identified Gaps** – The Self-Evaluation Report provides visualizations and tables that can help in the identification of gaps between an organization's current and target profiles. The following Self-Evaluation Report sections may be useful for identifying gaps:
  - **Section 3** can help identify high-level gaps, such as achievement of MIL targets by domain or the implementation of management activities across domains.
  - **Section 4** shows more precise information and could be used to review the achievement of practice-level implementation targets.
  - **Section 7** provides a listing of all practiced that received a response of *Partially Implemented* or *Not Implemented*.
- **Step 3: Prioritize and Plan** – The identification of gaps using the Self-Evaluation Report would feed into organizational processes to prioritize and address implementation gaps.
- **Step 4: Implement Plans and Periodically Reevaluate** – As organizations implement capabilities that have been determined to be most important,

repeating the self-evaluation process may help track progress in meeting MIL and implementation targets.

Figure 12 - Potential Approach for Using the C2M2 Model

3.6 Section 6 – Self-Evaluation Notes

This section contains a listing of all notes captured during the self-evaluation by order of domain and practice. Notes captured during a self-evaluation may include additional context regarding the selected implementation level or other considerations captured during the self-evaluation.

3.7 Section 7 – List of *Partially Implemented* and *Not Implemented* Practices

This section lists all practices that received a response of either *Largely Implemented* or *Fully Implemented*. The tables are ordered by MIL, then by practice to help facilitate the identification of practices that an organization may consider implementing to achieve a target MIL for a domain.

4. INTERPRETING THE SELF-EVALUATION RESULTS COMPARISON REPORT

4.1 Section 1 – Introduction

Section 1 includes the description of each self-evaluation that was entered during data set import.

4.2 Section 2 – MIL Achievement Comparison by Domain

Section 2 contains a high-level comparison of the MIL achieved in each domain for each of the self-evaluation data sets. This visualization provides insight into how MIL achievement is trending when comparing self-evaluations for a single function over a series of time or how MIL achievement compares between different functions.

4.3 Section 3 – Comparison of Practice Implementation by Domain

Section 3 contains summarized implementation responses for each C2M2 practice, grouped by domain for each imported self-evaluation. These visualizations may be helpful for organizations that have developed plans to address identified cybersecurity capability gaps by comparing self-evaluation results over a series of time. Alternatively, comparing the self-evaluation results for multiple functions would provide insight into areas where the cybersecurity capability diverges between the functions.

Each page contains a numbered listing of the self-evaluations that have been imported into the tool in the top left corner; these correspond with the numbers located on the X axis of the visualizations. The MIL achieved for the domain is listed at the bottom of each visualization.

4.4 Section 4 – Comparison of Practice Implementation by Objective

Section 4 contains a more granular view of practice implementation responses summarized at the objective level for each imported self-evaluation. Like the prior section, these visualizations may be helpful when evaluating progress in closing capability gaps for a single function or understanding how more specific groupings of cybersecurity activities compare between different functions.

Each page contains a numbered listing of the self-evaluations that have been imported into the tool in the top left corner; these correspond with the numbers located on the X axis of the visualizations.

4.5 Section 5 – Detailed Self-Evaluation Results Comparison

Section 5 contains the most granular comparison in this report. The implementation response for each practice can be compared across the imported self-evaluations. Tables in this section may be beneficial to review if implementation level targets are being achieved for specific practices.

At the beginning of the section, a numbered listing of the self-evaluations that have been imported into the tool is in the top left corner; these correspond with the numbers in the table headers.

This page left blank intentionally.